Implementing Directive dated September 29, 1978, issued through the Information Security Oversight Office.

Subpart 105–62.1—Classified Materials

§ 105–62.101 Security classification categories.

As set forth in Executive Order 12065, official information or material which requires protection against unauthorized disclosure in the interests of the national defense or foreign relations of the United States (hereinafter collectively termed ''national security'') shall be classified in one of three categories: Namely, Top Secret, Secret, or Confidential, depending on its degree of significance to the national security. No other categories shall be used to identify official information or material as requiring protection in the interests of national security except as otherwise expressly provided by statute. The three classification categories are defined as follows:

(a) *Top Secret.* Top Secret refers to that national security information which requires the highest degree of protection, and shall be applied only to such information as the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, intelligence sources and methods, and the compromise of vital national defense plans or complex cryptologic and communications systems. This classification shall be used with the utmost restraint.

(b) *Secret.* Secret refers to that national security information or material which requires a substantial degree of protection, and shall be applied only to such information as the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, and revelation of significant military plans or intelligence operations. This classification shall be used sparingly.

(c) *Confidential.* Confidential refers to other national security information which requires protection, and shall be applied only to such information as the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security.

§ 105–62.102 Authority to originally classify.

(a) *Top secret, secret, and confidential.* The authority to originally classify information as Top Secret, Secret, or Confidential may be exercised only by the Administrator and is delegable only to the Director, Information Security Oversight Office.

(b) *Limitations on delegation of classification authority.* Delegations of original classification authority are limited to the minimum number absolutely required for efficient administration. Delegated original classification authority may not be redelegated.

[47 FR 5416, Feb. 5, 1982]

§ 105–62.103 Access to GSA-originated materials.

Classified information shall not be disseminated outside the executive branch of the Government without the express permission of the GSA Security Officer except as otherwise provided in this § 105–62.103.

(a) *Access by historical researchers.* Persons outside the executive branch who are engaged in historical research projects, may be authorized access to classified information or material, provided that:

(1) A written determination is made by the Administrator of General Services that such access is clearly consistent with the interests of national security.

(2) Access is limited to that information over which GSA has classification jurisdiction.

(3) The material requested is reasonably accessible and can be located with a reasonable amount of effort.

(4) The person agrees to safeguard the information and to authorize a review of his or her notes and manuscript

for determination that no classified information is contained therein by signing a statement entitled ''Conditions Governing Access to Official Records for Historical Research Purposes.''

(5) An authorization for access shall be valid for a period of 2 years from the date of issuance and may be renewed under the provisions of this §105–62.103(a).

(b) *Access by former Presidential appointees.* Persons who previously occupied policymaking positions to which they were appointed by the President may not remove classified information or material upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information or material which they originated, received, reviewed, signed, or which was addressed to them while in public office, provided that the GSA element having classification jurisdiction for such information or material makes a written determination that access is consistent with the interests of national security, approval is granted by the GSA Security Officer, and the individual seeking access agrees:

(1) To safeguard the information,

(2) To authorize a review of his or her notes for determination that no classified information is contained therein, and

(3) To ensure that no classified information will be further disseminated or published.

(c) *Access during judicial proceedings.* Classified information will not normally be released in the course of any civilian judicial proceeding. In special circumstances however, and upon the receipt of an order or subpoena issued by a Federal court, the Administrator may authorize the limited release of classified information if he or she determines that the interests of justice cannot otherwise be served. Appropriate safeguards will be established to protect such classified material released for use in judicial proceedings.

(d) *Access to material in NARS custody.* The Archivist of the United States prepares procedures governing access to materials transferred to NARS custody. These procedures are issued by the Administrator of General Services in 41 CFR part 105–61.

(e) *Access by the General Accounting Office and congressional committees.* Classified information may be released to the General Accounting Office (GAO) and congressional committees when specifically authorized by the GSA Security Officer except as otherwise provided by law.

Subpart 105–62.2—Declassification and Downgrading

§105–62.201 Declassification and downgrading.

(a) *Authority to downgrade and declassify.* The authority to downgrade and declassify national security information or material shall be exercised as follows:

(1) Information or material may be downgraded or declassified by the GSA official authorizing the original classification, by a successor in capacity, by a supervisory official of either, or by the Information Security Oversight Committee on appeal.

(2) Downgrading and declassification authority may also be exercised by an official specifically authorized by the Administrator.

(3) In the case of classified information or material officially transferred to GSA by or under statute or Executive order in conjunction with a transfer of functions and not merely for storage purposes, GSA shall be deemed the originating agency for all purposes under these procedures including downgrading and declassification.

(4) In the case of classified information or material held in GSA not officially transferred under paragraph (a)(3) of this section but originated in an agency which has since ceased to exist, GSA is deemed the originating agency. Such information or material may be downgraded and declassified 30 calendar days after consulting with any other agencies having an interest in the subject matter.

(5) Classified information or material under the final declassification jurisdiction of GSA which has been transferred to NARS for accession into the Archives of the United States may be